Lower Bounds for Cover-Free Families

Ali Z. Abdi
Convent of Nazareth High School
Grade 12, Abas 7, Haifa

Nader H. Bshouty
Dept. of Computer Science
Technion, Haifa, 32000

April 1, 2015

Abstract

Let $\mathcal{F}$ be a set of blocks of a t-set X. $(X, \mathcal{F})$ is called (w, r)-cover-free family ($(w, r)-$CFF) provided that, the intersection of any w blocks in $\mathcal{F}$ is not contained in the union of any other r blocks in $\mathcal{F}$.

We give new asymptotic lower bounds for the number of minimum points t in a (w, r)-CFF when $w \le r = |\mathcal{F}|^{\epsilon}$ for some constant $\epsilon \ge 1/2$.

Keywords: Cover-Free Family, Lower Bound.

1 Introduction

Let $\mathcal{F}$ be a set of blocks (subsets) of a t-set X. $(X, \mathcal{F})$ is called (w, r)-cover-free family ($(w, r)-$CFF) provided that, for any w blocks $A_1, A_2, \dots, A_w \in \mathcal{F}$ and any other r blocks $B_1, B_2, \dots, B_r \in \mathcal{F}$ we have

$$\bigcap_{i=1}^{w} A_i \not\subseteq \bigcup_{j=1}^{r} B_j.$$

Since using De Morgan a $(w, r)-$CFF can be turned into $(r, w)-$CFF, throughout the paper we assume that $w \le r$. Cover-free families were first introduced in 1964 by Kautz and Singleton [5].

Let $N(n, (w, r))$ denote the minimum number of points $|X|$ in any (w, r)-CFF having $|\mathcal{F}| = n$ blocks. The best known lower bound for $N(n, (1, r))$ is [2, 4, 7]

$$N(n, (1, r)) = \Omega\left(\frac{r^2}{\log r} \log n\right) \tag{1}$$

when $r \le \sqrt{n}$ and $\Omega(n)$ when $r > \sqrt{n}$. The constant of the $\Omega()$ is asymptotically 1/2, 1/4 and 1/8, respectively. Stinson et. al, [8], proved that

$$N(n,(w,r)) \ge N(n-1,(w-1,r)) + N(n-1,(w,r-1)). \tag{2}$$

They then use it with (1) to prove two bounds. The first bound is

$$N(n,(w,r)) \ge \Omega\left(\frac{\binom{w+r}{w}(w+r)}{\log\binom{w+r}{w}}\log n\right) \tag{3}$$

when $r \le \sqrt{n}$, [8, 6], and

$$N(n,(w,r)) \ge \Omega\left(\frac{\binom{w+r}{w}}{\log(w+r)}\log n\right) \tag{4}$$

for any $r \le n$, [8]. To the best of our knowledge (4) is the best bound known when $\sqrt{n} \le r \le n$. D'yachkov et. al. breakthrough result, [3], implies that for $r \le \sqrt{n}$ and $r, n \to \infty$

$$N(n,(w,r)) = \Theta\left(\frac{\binom{w+r}{w}(w+r)}{\log\binom{w+r}{w}}\log n\right) \tag{5}$$

and for $r \ge \sqrt{n}$ and $r, n \to \infty$

$$N(n,(w,r)) \le O\left(\frac{r}{w}\cdot\frac{\binom{w+r}{w}}{\log(w+r)}\log n\right). \tag{6}$$

In this paper we give a new lower bound for (w,r)-CFF when $r > \sqrt{n}$. We combine the two techniques used in [8, 6] and [1] to give the following asymptotic lower bound.

Theorem 1. *For any $2 \le k \le w < r \le n/2$ and*

$$(n+k-1-w)^{\frac{k-1}{k}} \le r \le (n+k-w)^{\frac{k}{k+1}}$$

$$N(n,(w,r)) \ge \frac{k^k k!}{2(k+1)^{2k}}\frac{r^{w+1}}{(w+1)!\ln^k r} = \Omega\left(\frac{\sqrt{k}}{e^k}\cdot\frac{r^{w+1}}{(w+1)!\ln^{k+1} r}\log n\right)$$

and for

$$r = \Omega\left((n\log n)^{\frac{w}{w+1}}\right)$$

$$N(n,(w,r)) = \Theta\left(\binom{n}{w}\right).$$

Our bound is

$$\Theta\left(\frac{\sqrt{k}\cdot r}{w(e\ln r)^k}\right)$$

times greater than the previous bound in (4). In particular, when k is constant, our lower bound improves the bound in (4) to

$$N(n,(w,r)) \geq \Omega\left(\frac{r}{w\log^k r}\cdot\frac{\binom{w+r}{w}}{\log(w+r)}\log n\right). \tag{7}$$

A slightly better bound can be achieved when $(n+k-w)^{\frac{k}{k+1}} \leq r \leq (n+k-w)^{\frac{k}{k+1}}\ln^{1/(k+1)} n$.

For example, let $w=4$. The table in Figure 1 compares our results with the previous results (asymptotic values)

r	Previous Lower Bounds (3), (4)	Upper Bound [3]	Our Lower Bound
$r \leq n^{1/2}$	$r^5\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log r}$	——
$n^{1/2} \leq r \leq n^{2/3}$	$r^4\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log^3 r}$
$n^{2/3} \leq r \leq n^{3/4}$	$r^4\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log^4 r}$
$n^{3/4} \leq r \leq n^{4/5}$	$r^4\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log r}$	$r^5\frac{\log n}{\log^5 r}$
$n > r \geq (n\log n)^{4/5}$	r^4	n^4	n^4

Figure 1: Results for $w=4$.

2 First Lower Bound

In this section we prove

Lemma 1. *Let $w \leq r \leq n/2$. If*

$$r=\Omega\left((n\log n)^{\frac{w}{w+1}}\right)$$

then

$$N(n,(w,r))=\Theta\left(\binom{n}{w}\right). \tag{8}$$

Otherwise,

$$N(n,(w,r)) \geq \Omega\left(\left(\frac{r}{(w+1)\ln r}\right)^{w+1}\log n\right). \qquad (9)$$

Lemma 1 follows from the following

Lemma 2. *Let $\epsilon < 1$ be any constant. For $w \leq r \leq n/2$ we have*

$$N(n,(w,r)) \geq \min\left((1-\epsilon)\frac{w^w}{(w+1)^{2w+1}}\cdot\frac{r^{w+1}}{\ln^w r}\quad,\quad \epsilon\binom{n}{w}\right) \qquad (10)$$

Proof. Let $(X,\mathcal{F})$ be an optimal (w,r)-CFF. Let $\mathcal{F}=\{F_1,\ldots,F_n\}$, $|X| = N = N(n,(w,r))$ and assume without loss of generality that $X=[N]:=\{1,\ldots,N\}$. Define $v^{(i)}\in\{0,1\}^n$, $i=1,\ldots,N$ where $v_j^{(i)}=1$ if and only if $i\in F_j$. Let $V=\{v^{(i)}|i=1,\ldots,N\}$. Let V_0 be the set of $v^{(i)}$ of weight $wt(v^{(i)})$ (i.e., $\sum_j v_j^{(i)}$) equal to w. Let

$$m=\frac{(w+1)^2 n\ln r}{wr}$$

and consider the two sets $V_1=\{v^{(i)}\mid w<wt(v^{(i)})<m\}$ and $V_2=\{v^{(i)}\mid wt(v^{(i)})\geq m\}$. Obviously, $V=V_0\cup V_1\cup V_2$ is a partition of V. Suppose

$$|V_0|\leq\epsilon\binom{n}{w}$$

and

$$\max(|V_1|,|V_2|)\leq(1-\epsilon)\frac{w^w}{(w+1)^{2w+1}}\cdot\frac{r^{w+1}}{\ln^w r}.$$

Consider $W=\{(j_1,\ldots,j_w)\mid 1\leq j_1<\cdots<j_w\leq n\}$ and $W'\subset W$ the set of all $(j_1,\ldots,j_w)$ where no $v^{(i)}\in V_0$, $i=1,\ldots,N$, satisfies $v_{j_1}^{(i)}=\cdots=v_{j_w}^{(i)}=1$. Obviously,

$$|W'|=\binom{n}{w}-|V_0|\geq(1-\epsilon)\binom{n}{w}.$$

Fix an element $v\in V_1$ and randomly and uniformly choose $j=(j_1,\ldots,j_w)\in W'$. We have

$$\mathbf{Pr}_{j\in W'}[v_{j_1}=\cdots=v_{j_w}=1] \quad\leq\quad \frac{\binom{wt(v)}{w}}{|W'|}\leq\frac{\binom{m}{w}}{(1-\epsilon)\binom{n}{w}}.$$

Therefore, the expectation of the number of $v \in V_1$ for which $v_{j_1} = \cdots = v_{j_w} = 1$ is at most

$$\begin{aligned}
\frac{\binom{m}{w}|V_1|}{(1-\epsilon)\binom{n}{w}} &\le \frac{1}{1-\epsilon}\left(\frac{m}{n}\right)^w |V_1| \\
&\le \frac{1}{1-\epsilon}\frac{(w+1)^{2w}\ln^w r}{w^w r^w}\cdot(1-\epsilon)\frac{w^w}{(w+1)^{2w+1}}\cdot\frac{r^{w+1}}{\ln^w r} \\
&= \frac{r}{w+1}.
\end{aligned}$$

Therefore, there is $j' = (j'_1, \ldots, j'_w) \in W'$ such that the number of $v \in V_1$ that satisfies $v_{j'_1} = \cdots = v_{j'_w} = 1$ is $r_1 \le r/(w+1)$. Since the weight of every $v \in V_1$ is greater than w, we can choose r_1 new entries $j''_1, \ldots, j''_{r_1} \notin \{j'_1, \ldots, j'_w\}$ such that for every $v \in V_1$ where $v_{j'_1} = \cdots = v_{j'_w} = 1$ there is j''_ℓ such that $v_{j''_\ell} = 1$.

Now randomly and uniformly choose

$$r_2 := \left\lceil \frac{wr}{w+1} \right\rceil$$

distinct $k_1, \ldots, k_{r_2} \in [n]$. Let A be the event that $\{k_1, \ldots, k_{r_2}\} \cap \{j'_1, \ldots, j'_w\} \neq \emptyset$. The probability that A does not happen is

$$\frac{\binom{n-w}{r_2}}{\binom{n}{r_2}} \ge \frac{\binom{n-w}{r_2}}{2^w\binom{n-w}{r_2}} = \frac{1}{2^w}$$

Then

$$\begin{aligned}
\mathbf{Pr}[A \vee (\exists v \in V_2)\ v_{k_1} = \cdots = v_{k_{r_2}} = 0] &\le 1 - \frac{1}{2^w} + |V_2|\frac{\binom{n-m}{r_2}}{\binom{n}{r_2}} \\
&\le 1 - \frac{1}{2^w} + |V_2|\left(\frac{n-m}{n}\right)^{r_2} \\
&\le 1 - \frac{1}{2^w} + |V_2|e^{-\frac{mr_2}{n}}
\end{aligned}$$

and

$$\begin{aligned}
|V_2|e^{-\frac{mr_2}{n}} &\le (1-\epsilon)\frac{w^w}{(w+1)^{2w+1}}\cdot\frac{r^{w+1}}{\ln^w r}\cdot e^{-\frac{(w+1)^2\ln r}{wr}r_2} \\
&\le (1-\epsilon)\frac{w^w}{(w+1)^{2w+1}}\cdot\frac{r^{w+1}}{\ln^w r}\cdot e^{-(w+1)\ln r} \\
&= (1-\epsilon)\frac{w^w}{(w+1)^{2w+1}}\cdot\frac{1}{\ln^w r} \\
&< \frac{1}{2^w}
\end{aligned}$$

Therefore,

$$\mathbf{Pr}[A \vee (\exists v \in V_2)\ v_{k_1} = \cdots = v_{k_{r_2}} = 0] < 1.$$

Therefore, there is $\{k_1, \ldots, k_{r_2}\}$ such that $\{k_1, \ldots, k_{r_2}\} \cap \{j'_1, \ldots, j'_w\} = \emptyset$ and for every $v \in V_2$ there is $k_\ell \in \{k_1, \ldots, k_{r_2}\}$ where $v_{k_\ell} = 1$.

Now it is easy to see that there is no $v \in V$ where $v_{j'_1} = \cdots = v_{j'_w} = 1$, $v_{j''_1} = \cdots = v_{j''_{r_1}} = 0$ and $v_{k_1} = \cdots = v_{k_{r_2}} = 0$. This implies that

$$\bigcap_{i=1}^{w} F_{j'_i} \subseteq \bigcup_{i=1}^{r_1} F_{j''_i} \cup \bigcup_{i=1}^{r_2} F_{k_i}$$

which is a contradiction. □

3 The Second Bound

In this section we prove Theorem 1.

Lemma 3. *For any* $2 \le k \le w \le r \le n/2$ *and*

$$2 \le r \le (n+k-w)^{\frac{k}{k+1}}$$

$$N(n,(w,r)) \ge \frac{k^k k!}{2(k+1)^{2k}} \frac{r^{w+1}}{(w+1)! \ln^k r} = \Omega\left(\frac{r^{w+1}}{(w+1)! \ln^k r}\right).$$

Proof. We prove the lemma by induction on w.

From Lemma 2 the lemma holds for $w = k$. Now assume the bound holds for some w and every r that satisfies $r \le (n+k-w)^{\frac{k}{k+1}}$. We now prove the bound for $w+1$ and $r \le (n+k-w-1)^{\frac{k}{k+1}}$

$$\begin{aligned}
N(n,(w+1,r)) &\ge N(n-1,(w,r))) + N(n-1,(w+1,r-1)) && (11)\\
&\ge \sum_{j=1}^{r} N(n-r+j-1,(w,j)) && (12)\\
&\ge N(n-r,(w,1)) + \\
&\qquad \sum_{j=2}^{r} \frac{k^k k!}{2(k+1)^{2k}} \frac{j^{w+1}}{(w+1)! \ln^k j} && (13)\\
&\ge \frac{k^k k!}{2(k+1)^{2k}(w+1)! \ln^k r} \sum_{j=1}^{r} j^{w+1}\\
&\ge \frac{k^k k!}{2(k+1)^{2k}(w+1)! \ln^k r} \int_0^r x^{w+1}\,\mathrm{d}x\\
&\ge \frac{2k^k k!}{(k+1)^{2k}} \frac{r^{w+2}}{(w+2)! \ln^k r}
\end{aligned}$$

Here, inequality (11) comes from [8]. Inequality (12) follows from the fact that $N(n-r+1,(w+1,1)) \geq N(n-r,(w,1))$. Inequality (13) follows from the induction hypothesis since

$$\begin{aligned} j &= r-(r-j) \\ &\leq (n+k-w-1)^{\frac{k}{k+1}}-(r-j) \\ &\leq (n+k-w-1-(r-j))^{\frac{k}{k+1}} \\ &= ((n-r+j-1)+k-w)^{\frac{k}{k+1}}. \end{aligned}$$

□

References

[1] N. Alon, V. Asodi. Learning a Hidden Subgraph. *SIAM J. Discrete Math.* 18(4). pp. 697–712 (2005).

[2] A. G. D'yachkov and V. V. Rykov. Bounds on the length of disjunctive codes. *Problemy Peredachi Informatsii*, 18(3), pp. 7–13, (1982).

[3] A. G. D'yachkov, I. V. Vorobev, N. A. Polyansky, V. Yu. Shchukin. Bounds on the rate of disjunctive codes. Problems of Information Transmission. 50(1), pp. 27–56. (2014).

[4] Z. Füredi. On r-Cover-free Families. *J. Comb. Theory, Ser. A*, 73(1). pp. 172–173. (1996).

[5] W. H. Kautz and R. C. Singleton. Nonrandom binary superimposed codes, *IEEE Trans. Inform. Theory*. 10, pp. 363–377. (1964).

[6] X. Ma and R. Wei. On Bounds of Cover-Free Families. Designs, Codes and Cryptography, 32, pp. 303–321, (2004).

[7] M. Ruszinkó. On the Upper Bound of the Size of the r-Cover-Free Families. *J. Comb. Theory, Ser. A*. 66(2). pp. 302–310. (1994).

[8] D. R. Stinson, R. Wei and L. Zhu. Some New Bounds for Cover-Free Families. *Journal of Combinatorial Theory, Series A*. 90, pp. 224–234 (2000).